REMARKS

Claims 18, 21-22, 24-26, 28-30, 32-38, 40-41, and 45 are pending. Claims 18, 22, 35, 36, 37, 38, 40, 41, and 45 are amended. Claims 19, 20, 39, 42, 43, and 44 have been canceled. No new matter has been added.

The amendments are presented herein so as to expedite prosecution, and the original or any other claim scope is not conceded. Applicants reserve the right to pursue at a later date any previously pending or other broader or narrower claims that capture any subject matter supported by the present disclosure, including subject matter found to be specifically disclaimed herein or by any prior prosecution.

Interview Summary

Examiner James Nigh and the undersigned discussed the above application on March 3, 2011. The undersigned thanks the Examiner for his time and the professional and constructive manner with which the interview was conducted. Specifically, the Examiner and the undersigned discussed the nature of the invention recited in the claims, the references, and possible amendments to the claims. No agreement was reached.

Rejection Under 35 U.S.C. §101

The Office Action rejected claims 36-39 and 41-44 under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter.

Although Applicant respectfully disagrees with this rejection, Applicant has nevertheless amended the claims for the purposes of expediting prosecution. Applicant therefore respectfully requests that the 35 U.S.C. §101 rejection of claims 36-39 and 41-44 be withdrawn.

Rejections Under 35 U.S.C. §112

The Office Action rejected claims 37-40 under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement.

The Examiner states that "determining which one of a plurality of encrypted blocks of game code is to be executed..." and "attempting to authenticate the information..."of claims 37 and 40 are

not supported in the specification (Office Action, p. 7). Applicant respectfully disagrees with this statement. As the Examiner has noted, paragraph [0051] of the specification includes "decrypt[ing] only a specific portion or block of code/data from a group of code." Since each specific portion is encrypted with a certain key from a certain secure access module, then the gaming device with a certain secure access module must determine which block of code it can decrypt, given its specific secure access module and key. By virtue of having a secure access module containing a key for decrypting a specific portion or block of code/data from a group of code, the gaming device necessarily determines which block it can decrypt because the determined block is the only block the gaming device can decrypt, given its secure access module. In addition, paragraph [0057] of the specification recites "the method may include additional authentication steps..." If authentication steps are carried out, an attempt to authenticate is implied.

The Examiner also states that "sending to the gaming device the first key..." and "sending to the gaming device the second key..." of claim 37 are not supported (Office Action, p. 7). Claim 37 has been amended, thus rendering this rejection moot.

The Examiner also states that "sending the gaming device..." of claim 38 is new subject matter (Office Action, p. 7). Applicant respectfully disagrees with this statement. Paragraph [0042] of the specification recites "the encrypted code...when it is transmitted and stored at the gaming device..." Here, "transmit" is synonymous with "send." Therefore, "sending" the encrypted code to the gaming device is supported in the specification. Hence, "sending the game device..." of claim 38 is not new subject matter.

Dependent claims 38-39 were rejected based upon their dependency to 37. Therefore, Applicant submits that claim 38 is now in condition for allowance. Claim 39 has been canceled.

For the reasons discussed above, Applicant respectfully requests that the 35 U.S.C. §112 written requirement rejection of claims 37-40 be withdrawn.

The Office Action rejected claims 20 and 37-40 under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the enablement requirement.

The Examiner has rejected claim 20. However, claim 20 has now been canceled. Therefore, the rejection of claim 20 is moot.

The Examiner states that "determining which one of a plurality of encrypted blocks of game code is to be executed..." of claims 37 and 40 is not described in such a way to enable one skilled in the art to make or use the invention (Office Action, p. 8). However, as described above, by virtue of

having a secure access module containing a key for decrypting a specific portion or block of code/data from a group of code, the gaming device necessarily determines which block it can decrypt because the determined block is the only block the gaming device can decrypt, given its secure access module. Applicant notes that it is the gaming device, through its secure access module, that is recited in the claims to determine which block to execute, not an operator.

Dependent claims 38-39 were rejected based upon their dependency to 37. Therefore, Applicant submits that claim 38 is now in condition for allowance. Claim 39 has been canceled.

For the reasons discussed above, Applicant respectfully requests that the 35 U.S.C. §112 enablement requirement rejection of claims 37-40 be withdrawn.

The Office Action rejected claims 18-22, 28-30, and 32-45 under 35 U.S.C. §112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner states that "receiving from a remote device...code necessary to operate a game..." of claims 18, 22, 35, 36, 37, 40, 41, and 45 is indefinite because the claims do not recite within the claim as to whether this comprises the full extent of what is "necessary to operate a game" (Office Action, p. 9). Applicant respectfully disagrees with this statement. The claims recite that the "encrypted executable code" includes "code necessary to operate a game." The Examiner interprets this as "potentially encompassing unrecited elements" (Office Action, p. 9). However, the claims do not recite "*all* code necessary to operate a game," but rather just code that is necessary to operate a game. The claims do not encompass unrecited elements because it is clear that the code that is encrypted is necessary to operate a game, but it is not all that is necessary and need not be so. Other necessary components that are not encrypted code are not recited in the claims and hence, not claimed. The claims are clear because it recites that the encrypted code contains game code necessary to operate a game and does not need to recite all that is necessary to operate a game as posited by the Examiner.

The Examiner also states that "taking remedial action..." is indefinite for failing to claim the essential step of "receiving the authentication results" (Office Action, p. 10). Claim 18 has been amended in such a way as to render this rejection moot.

The Examiner also states that it is unclear how to authenticate the code without sending the actual code to the remote device (Office Action, pp. 10-11). Examiner appears to be saying that authentication of code by a remote device cannot be done unless the actual code is sent to the remote

device. Applicant respectfully disagrees and submits that authentication can be possible even if only "information relating to the code" is sent. In addition, information relating to the code could also encompass the code itself, thereby allowing authentication according to the Examiner's standards.

The Examiner states that "remedial"is a relative term (Office Action, p. 11). Applicant respectfully disagrees. Paragraph [0058] of the specification states that if the code is not authenticated, then the data is not used and "any necessary steps may be taken to ensure security of the gaming machine." It is quite clear that interpreting the claims in light of the specification would reveal that "remedial" refers to these "necessary steps."

The Examiner states that "decrypting" will also encompass "storing" (Office Action, p. 12) and hence an ambiguity is created as to whether an essential step has been omitted. While Applicant contends that "decrypting" does not encompass "storing," Claim 18 has been amended such that the rejection is now moot.

The Examiner has rejected claim 19 as being inconsistent with "...receiving...from the remote device a private key..." (Office Action, p. 12). Claim 18 has been amended and claim 19 has been canceled, thereby rendering the rejection moot.

The remaining §112 indefiniteness rejections are also traversed. However, in order to expedite prosecution, claims 36-38 and 41 have been amended accordingly and claims 39 and 42-44 have been canceled, thus rendering the rejections moot. Therefore, Applicant respectfully requests that the 35 U.S.C. §112 indefiniteness rejections be withdrawn.

Rejections Under 35 U.S.C. §103(a)

The Office Action rejected claims 18, 21, 33, 34, 36-40, and 45 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,645,077 to Rowe (hereinafter "Rowe") in view of U.S. Patent No. 6,978,367 to Hind et al. (hereinafter "Hind") and further in view of U.S. Patent No. 6,149,522 to Alcorn et al. (hereinafter "Alcorn").

The Office Action rejected claims 19, 20, 22, 24-26, 29, 30, and 35 under 35 U.S.C. §103(a) as being unpatentable over Rowe in view of Hind and Alcorn and further in view of U.S. Patent No. 5,991,399 to Graunke et al. (hereinafter "Graunke").

The Office Action rejected claim 28 under 35 U.S.C. §103(a) as being unpatentable over Rowe in view of Hind, Alcorn, and Graunke and further in view of U.S. Patent No. 6,226,749 to Carloganu et al. (hereinafter "Carloganu").

The Office Action rejected claim 32 under 35 U.S.C. §103(a) as being unpatentable over Rowe in view of Hind and Alcorn and further in view of Carloganu.

The Office Action rejected claims 41, 42, and 44 under 35 U.S.C. §103(a) as being unpatentable over Rowe in view of Hind.

The Office Action rejected claim 43 under 35 U.S.C. §103(a) as being unpatentable over Rowe in view of Hind and further in view of Graunke.

The rejections are traversed as follows.

Amended claim 18 recites as follows in pertinent part:

> (**Currently Amended**) A method of operating a gaming device configured to execute a decrypted executable game code, the method comprising:
>
> receiving at the gaming device from a remote device encrypted executable code for a plurality of games, the encrypted executable code including first game code necessary to operate a game on the gaming device in a first jurisdiction, the first game code encrypted with a first key associated with the first jurisdiction, and second game code necessary to operate a game on the gaming device in a second jurisdiction, the second game code encrypted with a second key associated with the second jurisdiction, the second game code not recoverable with the first key and the first game code not recoverable with the second key, wherein the first game code includes a first set of operating data including at least one of first audio data or first video data for generating the game on the gaming device in the first jurisdiction, and wherein the second game code includes a second set of operating data including at least one of second audio data or second video data for generating the game on the gaming device in the second jurisdiction;
>
> ...
>
> storing on the gaming device a secure access module, wherein the secure access module includes a private key associated with a local jurisdiction in which the gaming device is located, such that the private key need not be transmitted over a network;
>
> wherein when the private key is the first key, and the local jurisdiction is the first jurisdiction, decrypting by the gaming device the first game code according to the first key to recover the first game code and the first set of operating data as decrypted first game code and a decrypted first set of operating data, respectively;
>
> wherein when the private key is the second key, and the local jurisdiction is the second jurisdiction, decrypting by the gaming device the second game code according to the second key to recover the second game code and the second set of operating data as decrypted second game code and decrypted second set of operating data, respectively;
>
> ...
>
> executing the decrypted first or second game code on the gaming device using the decrypted first or second set of operating data when the decrypted first or second game code is authenticated by the remote device.

More notably, amended claim 18 recites "receiving at the gaming device...executable code for a plurality of games...including a first game...and second game...," wherein the gaming device is "configured to execute a decrypted executable game code." In addition, amended claim 18 also recites "storing on the gaming device a secure access module, wherein the secure access module includes a private key associated with a local jurisdiction in which the gaming device is located, such that the private key need not be transmitted over a network."

Rowe is directed toward a gaming terminal data repository and information distribution system. The Examiner states in the Office Action that Rowe discloses receiving executable code for a plurality of games, including a first game and a second game (Office Action, p. 15). However, claim 18 has been amended to recite "receiving at the gaming device" wherein the gaming device is "configured to execute a decrypted executable game code." While Rowe does disclose storing multiple games onto a game terminal data repository (GTDR), the GTDR is not the gaming device itself and cannot execute a decrypted executable game code. In order for the system in Rowe to execute code for a game, the game has to be downloaded first from the GTDR to a gaming terminal (Rowe, column 13:35-50). wherein the gaming device "is configured to execute a decrypted executable game code. The main purpose of Rowe is to utilize the GTDR to store multiple games and send a selected game to a gaming terminal. The claimed invention eliminates the use of a "middleman" and sends the executable code for the plurality of games to the gaming device directly. Therefore, Rowe does not teach or disclose "receiving at the gaming device...executable code for a plurality of games...including a first game...and second game..."

Hind is insufficient to cure the deficiencies of Rowe. Hind is directed towards selective data encryption for computer programs. While relevant to the encryption elements of claim 18, Hind does not teach or disclose receiving multiple executable code for a plurality of games at a gaming device as recited in amended claim 18. In addition, the combination of Rowe as the primary reference and Hind as a secondary reference does not yield the elements of amended claim 18. Since the main focus and advantage advertised in Rowe is the use of the GTDR, the GTDR cannot be left out of the combination of Rowe and Hind. Therefore, the combination of Rowe and Hind actually yields receiving executable code for a plurality of games at a GTDR, where the code is selectively encrypted. Then once a selected game has been selectively decrypted, the decrypted

game is sent to a gaming terminal for execution. Thus, the combination of Rowe and Hind is patentably distinguishable from the claimed invention.

Alcorn is used to teach authentication of game data. Alcorn does not cure the deficiencies described above for Rowe and Hind, taken alone or in combination.

Graunke is directed towards a method for securely distributing a conditional use private key to a trusted entity on a remote system. The Examiner uses Graunke to teach the "secure access module" as recited in claim 19, in other similar claims, and now in amended claim 18. However, the cited sections of Graunke teach transmitting the key wrapped in a "key module" so as not to "nakedly transmit[]" the key (Graunke, column 4:2-7). The "secure access module" as recited in the claims, by contrast is stored on the gaming device itself such that the private key need not be transmitted at all. The difference is that Graunke discloses a system where the key still needs to be transmitted, albeit wrapped in a "key module," but the claims recite a "secure access module" so that a key need not be transmitted at all. Therefore, Applicant respectfully submits that Graunke does not teach or suggest a security access module as recited in amended claim 18.

As discussed above, Rowe, Hind, and Alcorn, taken alone or in combination, do not disclose all elements of amended claim 18. Consequently, Applicant submits that claim 18 is patentably distinguishable over the prior art. Therefore, Applicant respectfully requests that the 35 U.S.C. §103(a) rejection of claim 18 be withdrawn.

Independent claims 22, 35, 36, 37, 40, 41, and 45 have been amended to incorporate similar features as amended claim 18. In addition, Graunke, as used by the Examiner in rejecting other claims for seemingly teaching the "secure access module," per the discussion above, does not teach the "secure access module" as recited in amended claim 18. Thus, Applicant submits that claims 22, 35, 36, 37, 40, 41, and 45 are patentable over the cited art at least for the reasons discussed above. Therefore, Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 22, 35, 36, 37, 40, 41, and 45 be withdrawn.

The dependent claims all depend from independent claims 18, 22, 35, 36, 37, 40, 41, and 45 and incorporate all features of their respective independent claims. Thus, Applicant respectfully submits that the dependent claims are patentable over the cited art at least for depending from a patentable independent claim. Therefore, Applicant respectfully requests that the 35 U.S.C. §103(a) rejection of the dependent claims be withdrawn.

Conclusion

Should the examiner believe that a telephone conference would expedite the prosecution of this application, applicant's attorney requests that the examiner contact him at the telephone number below.

Applicants hereby petition for any (additional) extension of time that may be required to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this amendment is to be charged to Deposit Account No. 504480 (Order No. IGT1P376US/P000227-001).

Respectfully submitted,
Weaver Austin Villeneuve & Sampson LLP

/William J. Egan, III/
William J. Egan, III
Reg. No. 28,411

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100